Enabling Warfighter Mission Assurance Through Effective Vulnerability Remediation

By Steve Muck

A component of the DON Critical Infrastructure Protection (CIP) Program is remediation of vulnerabilities identified by either an outside assessment team or as the result of a self-assessment conducted by the command. This is an integral part of Secretary of the Navy CIP Instruction 3501.1A and supports the Department of Defense Directive 3020.40, Defense Critical Infrastructure Program (DCIP). The following article describes a new DON CIP initiative in the area of remediation.

Providing vulnerability remediation training has been a goal of the Department of the Navy Critical Infrastructure Protection (DON CIP) Program for some time, a goal whose urgency has grown as the issues facing installation commanders have become more complex.

Funding, personnel, materiel, time — in some cases all of these — have made the decision of what and how to remediate difficult at best. In response, the DON CIP team has developed a Command Remediation Visit initiative that assists installation commanders in this area by providing on-site risk management based training and analytical guidance.

A major component of the Command Remediation Visit is the **"Remediation: Analysis, Strategy and Action Plan (ASAP)"** course, a training program developed specifically for DON regional and installation representatives.

Remediation training can occur at any time, but it is most effective when it occurs shortly after the completion of a vulnerability assessment. The first implementation of the CIP remediation initiative (at Naval Air Station Whidbey Island Wash., in September 2006) followed this preferred protocol by occurring shortly after a Chief of Naval Operations Integrated Vulnerability Assessment (CNO IVA), which was completed in August.

The DON CIP team presented the ***Remediation: ASAP*** training course to 12 senior Navy and civilian staff representatives from NAS Whidbey Island and various tenant commands. The class focused on training the installation staff to utilize the course's disciplined remediation analysis processes (see Figure 1), which were applied to a sample of the vulnerabilities identified during the August CNO IVA.

This instruction enabled the staff to evaluate and prioritize assessment findings and the remediation options available for each vulnerability identified. A product of the training was a set of proposed courses of actions created by class participants for remediating the assessment's more significant vulnerabilities.

This set of actions was briefed by the NAS Whidbey Island Executive Officer, Cmdr. Dan Brown, to the Commanding Officer, Capt. Syd Abernethy.

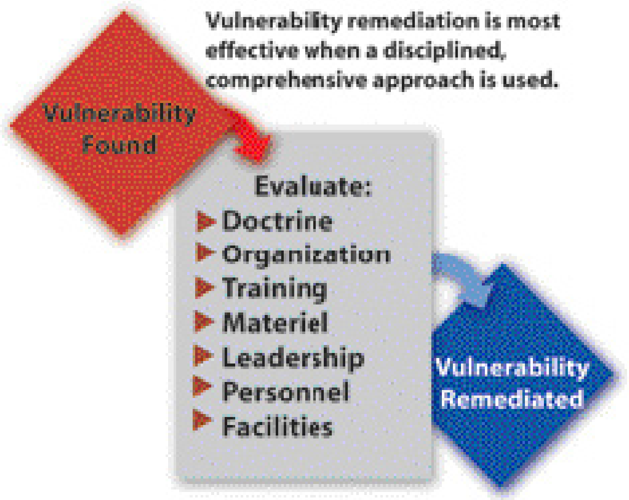

Figure 1. Training focused on a disciplined approach.

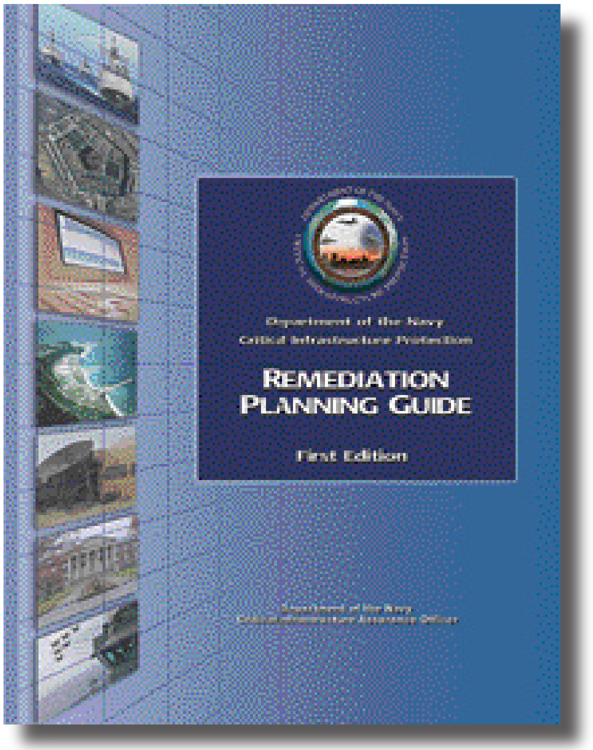
Department of the Navy
Critical Infrastructure Protection
REMEDIATION PLANNING GUIDE
First Edition
Department of the Navy
Critical Infrastructure Assurance Officer

Figure 2. DON Remediation Planning Guide.

An ongoing benefit is that with the understanding gained over two days of intense classroom training, the installation and tenant command staffs can now apply the ***Remediation: ASAP*** processes to the remaining assessment findings in order to develop a comprehensive remediation action plan.

Feedback from course participants was overwhelmingly positive, with most stating that their training experience produced a plan that was both viable and valuable. The structured methodology to work through vulnerabilities set the stage for implementation and gave users a tangible plan of action.

Reactions included comments such as: "The session encouraged out-of-the-box thinking that resulted in imaginative solutions ..."

"Using a cross-functional approach with non-subject matter experts having equal opportunity for input really helped us work toward smarter decisions …"

Capt. Abernethy said, "For us, it was a positive experience we would recommend to other installations."

Training Foundation and Key Tool: The Remediation Planning Guide

The CIP team developed the training from the concepts discussed in the DON Remediation Planning Guide, published in 2004 by the DON Chief Information Officer (CIO), as the DON Critical Infrastructure Assurance Officer (see Figure 2).

This planning document provides a methodology and plan of action that assists DON entities in developing vulnerability remediation strategies that balance resources and risk.

For example, the guide defines four factors critical

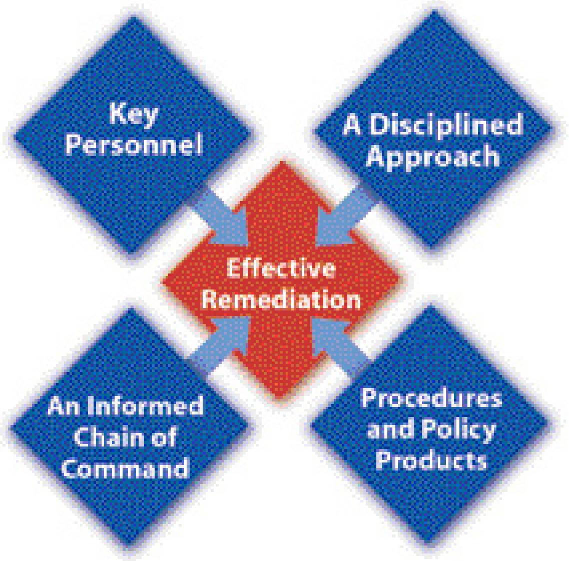

Figure 3 illustrates the four factors that are critical to successful remediation within a disciplined approach.

to successful remediation, as shown in Figure 3: (1) procedures/policy; (2) an informed chain of command; (3) key personnel; and (4) a disciplined approach. The first three factors are controlled by the command.

The ***Remediation: ASAP*** training course provides the disciplined approach necessary to develop and implement a successful remediation plan.

The effectiveness of the approach taught within the course depends on the involvement of key installation and tenant command personnel, the support of an informed chain of command and a thorough understanding of the particular policies and procedures applicable to the installation.

The goal of successful remediation is to reduce vulnerabilities while achieving maximum return on investment and focusing limited resources on the most essential assets.

Remediation can provide proactive protection against criminal and natural acts that threaten to disrupt mission accomplishment. Because proper remediation may actually thwart or minimize the chances of a terrorist attack, it makes sense to "harden" those assets believed critical to the warfighter's mission through remediation actions.

The DON CIP Program's Command Remediation Visit initiative is a valuable tool that supports mission assurance by promoting effective remediation strategies and plans.

To access CIP policy and guidance, go to the DON CIO Web site at http://www.doncio.navy.mil, click on the Project Teams tab, then click on Critical Infrastructure Protection.

CHIPS

Coalition Interoperability Reaches New Heights in RIMPAC 2006

Forty ships, six submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States engaged in seamless communications during RIMPAC 2006 …

By Lt. Cmdr. Vince Augelli, Lt. Cmdr. Dave Samara and Lt. Cmdr. George Haw

Commander, U.S. Third Fleet achieved unprecedented coalition interoperability during the latest Rim of the Pacific (RIMPAC) exercise. Scheduled by the Commander, U.S. Pacific Fleet, RIMPAC is a biannual multinational exercise conducted in the Hawaiian operating area. The exercise, conducted from June 26 through July 28, featured 40 ships, 6 submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States.

Cooperative Maritime Forces Pacific

The major advance in RIMPAC '06 was the introduction of the Combined Enterprise Regional Information Exchange System (CENTRIXS) community of interest called the Cooperative Maritime Forces Pacific (CMFP).

CMFP offered Web-browsing, e-mail, chat and the common operational picture over a secure network. While different security enclaves within CENTRIXS have been used in previous RIMPAC exercises, this was the first time that all participants had access to a common network.

A comparison between RIMPAC '04 and RIMPAC '06 will better illustrate this. The January-March 2005 edition of CHIPS featured an article *(available at http://www.chips.navy.mil/archives/05_Jan/web_pages/RIMPAC.htm)* describing the C4I architecture for RIMPAC 04. It included four different security enclaves for coalition releasability: CENTRIXS FOUR EYES – used by U.S., U.K., Canadian and Australian forces; CENTRIXS-J – used by U.S. and Japanese forces; CENTRIXS-R – used by U.S., South Korean and Chilean forces; and SIPRNET – used by U.S. forces.

For these four different security enclaves partial interoperability was achieved through the use of air-gapping, replication and a high assurance mail guard.

Of note, only the exercise's Task Force Commander/Combined Forces Maritime Component Commander (CFMCC) ashore in Pearl Harbor enjoyed access to all four enclaves. All other participants were dependent on the redistribution of information from this central node. While cleverly done, time delays were unavoidable.

In contrast, CENTRIXS Cooperative Maritime Forces Pacific was accessible to CFMCC headquarters, the outlying shore sites including all component commanders and commanders of maritime task forces, and every U.S. and coalition ship in the entire exercise. Information that was seen at Pearl Harbor was available afloat at the same time. This led to an unprecedented level of operational execution and planning.

CMFP Provides Unprecedented Interoperability

CMFP is a new community of interest in the existing CENTRIXS Global Counterterrorism Task Force (GCTF) security enclave. It was developed by Mr. Bob Stephenson, chief technology officer for command, control, communications, computers and intelligence operations at the Space and Naval Warfare Systems Command, and Mr. Tim Gannon, a division head from the Naval Network Warfare Command. The CMFP was used on a large scale for the first time during RIMPAC '06.